Computer Network Lab

Assessment # 02

Submitted By
QASIM ALI (20P-0070)
Submitted to : Hurmat Hidayat
(INSTRUCTOR CS)

DEPARTMENT OF COMPUTER SCIENCE

FAST NATIONAL UNIVERSITY OF COMPUTER AND EMERGING SCIENCES, PESHAWAR

Session 2020-2024

1: Introduction: Explain why wireless security matters for Wi-Fi networks.

Ans:

What is wireless security:

Wireless security is the process of protecting your Wi-Fi network from unauthorized access and malicious attacks. Your Wi-Fi network is like a neighborhood, and wireless security is like putting up gates and fences to keep out unwanted visitors.

Introduction:

In today's digital world, Wi-Fi has become an essential part of our lives. We use it to connect to the internet, work from home, and stream our favorite shows. However, Wi-Fi networks are also vulnerable to cyberattacks, which can put our data and devices at risk. That's why wireless security matters.

Wireless security is of paramount importance for Wi-Fi networks due to the inherent vulnerabilities associated with wireless communication. Wi-Fi networks transmit data over the airwaves, making them susceptible to various security threats that can compromise the confidentiality, integrity, and availability of information. Understanding why wireless security matters is crucial for maintaining the privacy and reliability of Wi-Fi networks.

Why Wireless Security Matters

Wireless security is important because it protects your data and devices from unauthorized access and malicious attacks. Without proper security, your Wi-Fi network is vulnerable to a range of threats, including:

- **Eavesdropping:** Attackers can intercept data that is being transmitted over your Wi-Fi network, including sensitive information like passwords, credit card details, and personal files.

- **Man-in-the-middle (MITM) attacks:** Attackers can position themselves between your device and the Wi-Fi network, intercepting and modifying data in transit. This can be used to steal information, redirect you to fake websites, or inject malware onto your device.

- **Unauthorized access**: Attackers can gain unauthorized access to your Wi-Fi network and use it to connect to your devices, steal data, or launch attacks against other networks.

- **Malware infections:** Attackers can distribute malware through your Wi-Fi network, infecting your devices with viruses, ransomware, or other harmful software.

- **Denial-of-service (DoS) attacks:** Attackers can flood your Wi-Fi network with traffic, making it unavailable to legitimate users.

- **War driving:** Attackers can use war driving to locate and map unsecured Wi-Fi networks, making them easier to target for attacks.

2-Basic Concepts: Describe the core ideas of wireless security in an easy-to-understand Way?

Ans: The core ideas of wireless security revolve around protecting wireless communication networks from unauthorized access, data breaches, and other security threats. Here are some key concepts and measures associated with wireless security:

1. **Encryption**: Use strong encryption protocols to secure the data transmitted over the wireless network. This ensures that even if someone intercepts the data, they cannot easily decipher it without the appropriate encryption key.

2. **Authentication**: Implement robust authentication mechanisms to ensure that only authorized users and devices can access the wireless network. This can include password-based authentication, certificate-based authentication, and other multi-factor authentication methods.

3. **Access Control:** Define and enforce access control policies to restrict access to the network and its resources. This involves setting permissions and privileges for different users and devices to prevent unauthorized access.

4. **Firewalls**: Employ firewalls to monitor and control incoming and outgoing network traffic. Firewalls act as a barrier between a trusted internal network and untrusted external networks, helping to prevent unauthorized access and protect against malicious activities.

5. Intrusion Detection and Prevention Systems (IDPS): Implement systems that can detect and respond to potential security threats. These systems monitor network and/or system activities for malicious actions or security policy violations and can take action to prevent or mitigate these threats.

6**. Regular Security Audits:** Conduct regular security audits to identify vulnerabilities in the wireless network. This involves assessing the network architecture, configurations, and policies to ensure they align with best practices and security standards.

7. **Firmware/Software Updates:** Keep wireless devices and network infrastructure up to date with the latest firmware and software updates. This helps patch security vulnerabilities and ensures that the network is protected against known exploits.

8. **Wireless Intrusion Prevention Systems (WIPS):** Deploy WIPS to monitor and mitigate unauthorized access points and other wireless security threats. WIPS can detect and respond to rogue access points and other suspicious activities in the wireless environment.

9. **Physical Security:** Protect physical access to wireless infrastructure, such as routers and access points, to prevent tampering or unauthorized installation of malicious devices.

10. **User Education and Awareness**: Educate users about security best practices, including the importance of strong passwords, avoiding public Wi-Fi risks, and recognizing social engineering attacks.

3-Types of Security: Introduce at least three common wireless security protocols like WEP, WPA, WPA2, or WPA3.

Ans: WEP (Wired Equivalent Privacy):

WEP (Wired Equivalent Privacy) was one of the first wireless security protocols developed to provide a level of security comparable to wired networks. It uses a static encryption key to protect data during transmission. However, WEP has significant security vulnerabilities and is now considered highly insecure. Its encryption can be easily cracked, and it is susceptible to various attacks, making it inadequate for modern wireless security needs.

Security Concerns of WEP:

- Static encryption key: WEP uses a static encryption key that is shared by all devices on the network. This makes it easy for attackers to intercept and decrypt data.
- Weak encryption algorithm: WEP uses the RC4 encryption algorithm, which is known to be weak and can be easily broken.
- Susceptibility to various attacks: WEP is susceptible to a variety of attacks, including eavesdropping, man-in-the-middle attacks, and replay attacks.

Recommendations for WEP:

- Do not use WEP for any new networks.
- Upgrade to a more secure protocol, such as WPA2 or WPA3, as soon as possible.
- Disable WEP on all of your devices.

WPA (Wi-Fi Protected Access):

WPA (Wi-Fi Protected Access) was introduced as an improvement over WEP to address its security weaknesses. WPA uses a stronger encryption algorithm called TKIP (Temporal Key Integrity Protocol) and introduces dynamic keys for each session. WPA provides better security than WEP, but it also has some vulnerabilities. It was a transitional security protocol and served as a bridge between the insecure WEP and the more robust WPA2.

Security Features of WPA:

- TKIP encryption: WPA uses TKIP encryption, which is a stronger encryption algorithm than the RC4 algorithm used in WEP.
- Dynamic keys: WPA uses dynamic keys that are generated for each session. This makes it more difficult for attackers to intercept and decrypt data.

Security Concerns of WPA:

- Vulnerabilities in TKIP encryption: TKIP encryption is not without its vulnerabilities. Some attacks have been discovered that can exploit weaknesses in TKIP.

- Limited adoption: WPA was not as widely adopted as WEP, which made it more vulnerable to attacks.

Recommendations for WPA:

- Do not use WPA for any new networks.
- Upgrade to WPA2 or WPA3 as soon as possible.
- Disable WPA on all of your devices.

WPA2 (Wi-Fi Protected Access 2):

WPA2 represents a significant enhancement in wireless security. It utilizes the Advanced Encryption Standard (AES) for encryption, which is considered highly secure. WPA2 replaced TKIP with AES-CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). WPA2 is widely adopted and provides strong protection against various attacks. However, it is not without flaws, and vulnerabilities such as KRACK (Key Reinstallation Attack) have been discovered, prompting the development of even more secure protocols.

Security Advancements of WPA2:

- AES encryption: WPA2 uses AES encryption, which is a very strong encryption algorithm.
- AES-CCMP protocol: WPA2 uses the AES-CCMP protocol, which is more secure than the TKIP protocol used in WPA.
- Strong authentication: WPA2 uses strong authentication mechanisms to prevent unauthorized access to the network.

Security Concerns of WPA2:

- Vulnerabilities like KRACK: Vulnerabilities such as KRACK have been discovered in WPA2. These vulnerabilities can be exploited by attackers to gain access to the network and decrypt data.
- Limited protection against password brute-force attacks: WPA2 is not as resistant to password brute-force attacks as WPA3.

Recommendations for WPA2:

- WPA2 is still a relatively secure protocol and can be used for most networks.
- However, it is important to keep your WPA2 password strong and complex.
- You should also consider upgrading to WPA3 as soon as possible.

WPA3 (Wi-Fi Protected Access 3):

WPA3 is the latest iteration of wireless security protocols, designed to address the shortcomings of WPA2. It introduces several security enhancements, including individualized data encryption for improved privacy and protection against brute-force attacks. WPA3 strengthens the security of Wi-Fi networks by introducing features like Simultaneous Authentication of Equals (SAE), which provides a more resilient key exchange mechanism. WPA3 is designed to be more resistant to various attacks, providing a higher level of security compared to its predecessors.

Key Security Improvements of WPA3:

1. Individualized Data Encryption: WPA3 employs individualized data encryption, ensuring that each device connected to the network has its own unique encryption key. This significantly enhances privacy and protection against brute-force attacks, making it more difficult for attackers to intercept and decrypt data.
2. Enhanced Key Exchange Mechanism: WPA3 introduces Simultaneous Authentication of Equals (SAE), a more resilient key exchange mechanism that replaces the Pre-Shared Key (PSK) method used in WPA2. SAE provides stronger protection against offline dictionary attacks, where attackers attempt to guess the network password by trying various combinations without further network interaction.
3. Forward Secrecy: WPA3 incorporates forward secrecy, ensuring that the compromise of a long-term key does not compromise the secrecy of past or future communications. This means that even if an attacker gains access to the long-term key, they cannot decrypt previously exchanged data or predict future encryption keys.
4. Protection Against Weak Passwords: WPA3 is designed to be more resilient against weak passwords, making it less vulnerable to password guessing attacks. It provides better protection even when users choose passwords that fall short of typical complexity recommendations.

Additional WPA3 Features:

- Opportunistic Wireless Encryption (OWE): OWE provides a simplified and secure way to connect devices that do not have a pre-shared key, such as smart home appliances and Internet of Things (IoT) devices.
- Suite B Cryptography: WPA3 supports Suite B cryptography for highly sensitive data markets, such as government and financial institutions, offering even stronger encryption algorithms.

Overall, WPA3 represents a significant advancement in wireless security, providing a more robust and secure foundation for protecting Wi-Fi networks against a wide range of threats. As devices that support WPA3 become more widely available, it is recommended to upgrade your network to WPA3 to ensure the highest level of protection.

4- Compare and Contrast: Highlight the pros and cons of each security protocol in a straightforward manner.

Ans: WEP (Wired Equivalent Privacy):

Pros:

1. Easy to set up and configure.
2. Widely supported on older devices.

Cons:

1. **Weak Security**: WEP has known vulnerabilities, and its encryption can be easily cracked.
2. **Static Keys:** The use of static keys makes it susceptible to various attacks.
3. **Obsolete**: Considered obsolete and insecure for modern wireless networks.

WPA (Wi-Fi Protected Access):

Pros:

1. **Improved Security**: Stronger encryption compared to WEP (uses TKIP).
2. **Dynamic Keys**: Utilizes dynamic keys for each session, enhancing security.

Cons:

1. **Vulnerabilities**: While an improvement, WPA has vulnerabilities, and some attacks can compromise its security.
2. **Transitionary**: Considered a transitional solution as it was later succeeded by WPA2.

WPA2 (Wi-Fi Protected Access 2):

Pros:

1. **Strong Security**: Uses AES encryption, considered highly secure.
2. **Robust Key Management**: More secure key management with CCMP.
3. **Widely Adopted**: Widely adopted and compatible with a broad range of devices.

Cons:

1. **Vulnerabilities**: Vulnerabilities have been discovered over time (e.g., KRACK attack).
2. **Aging Standard:** While still widely used, it's an aging standard, and newer protocols aim to address its limitations.

WPA3 (Wi-Fi Protected Access 3):

Pros:

1. **Enhanced Security**: Provides stronger security features, including individualized data encryption.
2. **Protection Against Brute-Force:** Improved protection against brute-force attacks.
3. **Simplified Configuration**: Supports Simultaneous Authentication of Equals (SAE) for a more secure key exchange.

Cons:

1. **Adoption Challenges**: Adoption may be slower due to the need for compatible hardware and devices.
2. **Compatibility**: Newer devices may be required to fully leverage WPA3 features.

It's important to note that security protocols evolve, and new vulnerabilities may be discovered over time. Therefore, it's recommended to use the latest and most secure protocols available, such as WPA3, when setting up or upgrading wireless networks. Additionally, network security should not rely solely on the encryption protocol but should also include other measures such as strong authentication, access control, and regular security updates.

5-Real-Life Examples: Share simple instances where these security protocols are used, like in homes or cafes.

Ans:

1. Home Network:

- WEP: Imagine a scenario where a person sets up a basic home Wi-Fi network using an older router that only supports WEP. This person may not be overly concerned about security but wants to have a password to prevent neighbors from freely accessing the internet.

- WPA/WPA2: A family with multiple devices and a moderate level of security consciousness sets up their home Wi-Fi using WPA or WPA2. They choose a strong, unique passphrase and configure their router to use WPA/WPA2 encryption to protect their data.

- WPA3: A tech-savvy individual with the latest router and devices decides to implement WPA3 at home for the enhanced security features, especially individualized data encryption. This person values the additional protection against potential security threats.

2. Cafe or Public Wi-Fi:

- WEP: Some smaller cafes or public spaces might still use older routers that support only WEP due to hardware limitations. Users connecting to these networks may have a basic level of protection, but they should be aware that WEP is not very secure.

- WPA/WPA2: More modern and secure cafes or public Wi-Fi hotspots are likely to use WPA or WPA2 encryption. Users connecting to these networks can have confidence in the encryption strength and protection against common attacks.

- WPA3: In cutting-edge or security-conscious establishments, especially as technology evolves, you might find WPA3 implemented to provide the highest level of security for customers connecting to the Wi-Fi network.

3. Enterprise Environment:

-WEP/WPA/WPA2: In older corporate environments, you might find a mix of security protocols. Some legacy devices or systems might only support WEP or WPA, while newer infrastructure might use WPA2 for enhanced security.

-WPA3: As enterprises upgrade their network infrastructure, they may transition to WPA3 to take advantage of its improved security features, especially in environments where protecting sensitive data is paramount.

Note:
These examples illustrate how different wireless security protocols are applied in various real-life settings, based on factors such as the level of security awareness, the age of the equipment, and the specific security needs of the users or organizations involved. It's important for individuals and businesses to assess their security requirements and choose the most suitable and secure wireless security protocol accordingly.

6-Future Trends: Mention any new developments in wireless security, but keep it simple.

Ans: Here are some new developments in wireless security:

1. **Physical-layer security:** This is an emerging field of security that focuses on using the physical properties of wireless signals to protect data. For example, researchers are developing methods to use noise to jam attackers or to use beamforming to focus signals on legitimate devices and away from attackers.
2. **Artificial intelligence (AI) and machine learning (ML):** AI and ML are being used to develop new security tools that can detect and prevent attacks in real time. For example, AI-powered systems can analyze network traffic to identify anomalies that may indicate an attack.
3. **Blockchain:** Blockchain is a distributed ledger technology that can be used to create tamper-proof records of wireless transactions. This could be used to improve the security of Wi-Fi networks by making it more difficult for attackers to forge or modify data.
4. **Internet of Things (IoT) security:** As the number of IoT devices grows, so does the need for secure wireless communication. Researchers are developing new security protocols and techniques to protect IoT devices from attacks.
5. **Zero-trust security**: Zero-trust security is a security model that assumes that no user or device is safe, and that all access to resources must be explicitly granted. This is becoming increasingly important for wireless security, as attackers are increasingly targeting wireless networks to gain access to sensitive data.

Etc.